Listing of the Claims:

1. (Currently amended) A ~~proxy~~ method comprising:

receiving encrypted data at a proxy from a client over an unsecure network wherein the receiving completes a first hop and the proxy is an ending point of a first communication associated with the first hop;

decrypting the encrypted data into decrypted data;

examining the decrypted data for security purposes;

re-encrypting the examined decrypted data; and

sending the re-encrypted data from the proxy to an origin server over a given network wherein the sending starts a second hop and the origin server is an ending point of a second communication associated with the second hop.

2. Canceled

3. Canceled

4. (Currently amended) The ~~proxy~~ method of claim 1, wherein the given network is a secure network.

5. (Currently amended) The ~~proxy~~ method of claim 4, wherein the sending is in accordance with one of the hypertext transport protocol (HTTP), the post office protocol (POP), the wireless access protocol (WAP), or the Internet messaging access protocol (IMAP).

6. (Currently amended) The ~~proxy~~ method of claim 1, wherein the given network is one of the unsecure network and a second unsecure network.

7. (Currently amended) The ~~proxy~~ method of claim 1, wherein the receiving is within a secure socket layer (SSL) session.

8. (Currently amended) The ~~proxy~~ method of claim 1, wherein the unsecure network is the Internet.

9. (Currently amended) The ~~proxy~~ method of claim 1, wherein the origin server is an effective origin server.

10. (Currently amended) The ~~proxy~~ method of claim 1, wherein the client is an effective client.

11. Canceled

12. (Currently amended) The ~~proxy~~ method of claim 1, wherein the method is performed by a firewall within the given network.

13. (Currently amended) A computer-readable medium having a computer program stored thereon for execution by a processor to perform the ~~proxy~~ method of claim 1.

14. (Previously presented) A proxy method comprising:

receiving unencrypted data from a client over a secure network;

examining the unencrypted data for security purposes; and,

in response to the examining yielding that the unencrypted data does not present a security risk:

encrypting the unencrypted data into encrypted data;

sending the encrypted data to an origin server over an unsecure network.

15. Canceled

16. (Previously presented) The proxy method of claim 14, wherein the unencrypted data is received from the client over the secure network in accordance with one of the post office protocol (POP), the Internet messaging access protocol (IMAP), the hypertext transport protocol (HTTP), or the wireless access protocol (WAP).

17. (Previously presented) The proxy method of claim 14, wherein the sending is within a secure socket layer (SSL) session.

18. (Previously presented) The proxy method of claim 14, wherein the secure network is a carrier network.

19. (Previously presented) The proxy method of claim 14, wherein the unsecure network is the Internet.

20. (Previously presented) The proxy method of claim 14, wherein the client is a thin client.

21. (Previously presented) The proxy method of claim 14, wherein the client is one of a: personal digital assistant (PDA) device, a laptop computer, a notebook computer, or a wireless phone.

22. (Previously presented) The proxy method of claim 14, wherein the secure network is one of a wireless network or a wired network.

23. (Previously presented) The proxy method of claim 14, wherein the client is an effective client.

24. (Previously presented) The proxy method of claim 14, wherein the origin server is an effective origin server.

25. Canceled

26. (Previously presented) The proxy method of claim 14, wherein the method is performed by a firewall within the secure network.

27. (Previously presented) A computer-readable medium having a computer program stored thereon for execution by a processor to perform the method proxy of claim 14.

28. (Currently amended) A system comprising:

a client to send encrypted data over an unsecure network and be a starting point of a first hop;

a proxy within a secure network to receive the encrypted data, decrypt the encrypted data into decrypted data, perform a test relative to the decrypted data, and send the decrypted data over the secure network in response to the test yielding a particular response wherein the proxy is an ending point of a first communication associated with the first hop and a starting point of a second communication associated with a second hop; and,

an origin server within the secure network to receive the decrypted data and be an ending point of the second communication associated with the second hop.

29. (Previously presented) The system of claim 28, wherein the client is an effective client comprising:

a second client within a second secure network to send unencrypted data over the second secure network; and,

a second proxy within the second secure network to receive the unencrypted data, encrypt the unencrypted data into the encrypted data, perform a second test relative to the unencrypted data, and send the encrypted data over the unsecure network in response to the second test yielding a second particular response.

30. (Previously presented) The system of claim 28, wherein the client is an effective client comprising:

a second client to send second encrypted data over the unsecure network in an additional hop; and,

a second proxy to receive the second encrypted data, decrypt the second encrypted data into second decrypted data, perform a second test relative to the second decrypted data, encrypt the second decrypted data into the encrypted data, and send the encrypted data over the unsecure network in response the second test yielding a second particular response.

31. (Previously presented) A system comprising:

a client to send unencrypted data over a secure network;

a proxy within the secure network to receive the unencrypted data, perform a test relative to the unencrypted data, encrypt the unencrypted data into encrypted data, and send the encrypted data over an unsecure network in response to the test yielding a particular response; and,

an origin server to receive the encrypted data.

32. (Previously presented) The system of claim 31, where the origin server is an effective origin server comprising:

a second proxy within a second secure network to receive the encrypted data, decrypt the encrypted data into decrypted data, and send the decrypted data over the second secure network; and,

a second origin server within the second secure network to receive the decrypted data.

33. (Currently amended) A proxy comprising:

one or more communication components enabling the proxy to communicate over a first network and a second network;

a processor; and,

a computer-readable medium having a computer program stored thereon for execution by the processor to:

receive data that is originally encrypted or unencrypted from a client over the first network as part of a first hop wherein the proxy is an ending point of a first communication associated with the first hop,

decrypt the data where the data was originally encrypted,

perform a test relative to the data,

in response to the test yielding a particular result, send the data as part of a second hop unencrypted to an origin server over the second network where the data was originally encrypted, or send the data as part of the second hop unencrypted or encrypted to the origin server over the second network where the data was originally unencrypted wherein the proxy is a starting point of a second communication associated with the second hop.

34. (Original) The proxy of claim 33, wherein the first network is a secure network.

35. (Previously presented) The proxy of claim 33, wherein the second network is an unsecure network, such that sending the data to the origin server over the second network comprises first encrypting the data.

36. (Original) The proxy of claim 33, wherein the second network is a secure network.